REMARKS

Claims 1-16 and 18-50 are pending in the application. Claims 1-9, 12-16, 18-20, 23-31, 34-42, and 45-48 are rejected under 35 U.S.C. § 102(e) as anticipated by U.S. Patent No. 5,870,470 granted to Johnson et al. and claims 10, 11, 21, 22, 32, 33, 43, 44, 49 and 50 are rejected under 35 U.S.C. § 103(a) as unpatentable over Johnson and further in view of U.S. Patent No. 6,031,911 granted to Adams et al.

Applicants' representative thanks the Examiner for granting an in-person Interview in this case, which is scheduled to be held on July 8, 2004.

1. Rejection of claims 1-9,12-16, 18-20, 23-31, 34-42, and 45-48

Applicants respectfully traverse the rejection of claims 1-9,12-16, 18-20, 23-31, 34-42, and 45-48 under 35 U.S.C. § 102(e) as being anticipated by Johnson. Claim 1 is patentable at least because Johnson does not teach each and every limitation of claim 1. Specifically, Johnson does not teach an encryption apparatus including means for removing an influence of a mask a from a ciphertext before the ciphertext is output. The Examiner continues to maintain his position that Johnson teaches the subject matter of claim 1. In particular, the Examiner in the "Response to Arguments" section primarily relies on his characterization of Figure 2 of Johnson to conclude that Johnson teaches an encryption apparatus including means for removing an influence of a mask a from a ciphertext before the ciphertext is output. (December 29, 2003 Office Action, page 2). Applicants respectfully disagree with the Examiner's interpretation of Figure 2 of Johnson at least for the following reasons.

With respect to Figure 2, Johnson teaches the following. An unmasked key block is divided into two parts: Part A (as shown in block 202) and Part B (as shown in block 204). Considering the processing of Part B first, an XOR operation is performed only

once between MASK 2 (block 216) and Part B in block 218 of Figure 2. This generates Masked Part B, as shown in block 220. Applicants note that MASK 2 is generated by applying a second generator function (G2) to Intermediate Part A, which in turn is generated by performing an XOR operation between MASK 1 (block 208 of Figure 2) and Part A. (Figure 2). As a result, Masked Part B is influenced by both MASK 1 and MASK 2. But, MASK 2 does not remove the influence of MASK 1, as alleged by the Examiner. Thus, Applicants respectfully submit that for at least this reason Johnson does not teach an encryption apparatus including means for removing an influence of a mask a from a ciphertext before the ciphertext is output.

Indeed, as shown in Figure 7 of Johnson, after the decryption process, unmasking procedure 630, which is the inverse of masking procedure 120 of Figure 2, is applied to Masked Part A and Masked Part B. (col. 6, ll. 44-48, Figure 7). As part of this process, Part A is generated by reversing the process applied in Figure 2 to Part A and similarly Part B is generated by reversing the process applied in Figure 2 to Part B. (Figure 7). The process shown in Figure 7 is performed after the decryption process of Figure 6. Consequently, any mask removal as part of this process results in processing of plaintext and not ciphertext. Thus, for at least this additional reason, Johnson does not teach an encryption apparatus including means for removing an influence of a mask a from a ciphertext before the ciphertext is output.

Considering next the processing of Part A, a first mask (MASK 1, 208 of Figure 2) is calculated using a first generator function (G1) on Part B. (col. 4, ll. 63-66). Next, an XOR operation is performed on Part A with MASK 1 in block 210 of Figure 2 (col. 5, ll. 1-5). This results in the generation of Intermediate Part A.

Next, an XOR operation is performed on Intermediate Part A and another mask (MASK 3, 224 of Figure 2). (col. 4, ll. 12-17). This results in the generation of Masked Part A (block 228 of Figure 2). In this respect, Applicants note that MASK 1 is a hashed value of Part B and MASK 3 is a hashed value of Masked Part B, which in turn is generated by performing an XOR operation on Part B and MASK 2 (block 218 of Figure 2). Thus, MASK 3 is influenced by both MASK 1 and MASK 2. Application of MASK 3 in an XOR operation to Intermediate Part A does not remove the influence of MASK 1 and MASK 2 because XOR is merely modulo 2 addition. Thus, the influence of MASK 1 and MASK 2 remains. Indeed, Masked Part A is influenced by all three masks: MASK 1, MASK 2, and MASK 3. Thus, Applicants respectfully submit that Johnson does not teach an encryption apparatus including means for removing an influence of a mask a from a ciphertext before the ciphertext is output.

Further, as discussed above, Part A is generated by reversing the process applied in Figure 2 to Part A. (Figure 7). The process shown in Figure 7 is performed after the decryption process of Figure 6. Consequently, any mask removal as part of this process results in processing of plaintext and not ciphertext. Thus, for at least this additional reason, Johnson does not teach an encryption apparatus including means for removing an influence of a mask a from a ciphertext before the ciphertext is output.

Claims 4, 8, and 9 depend from claim 1 and thus are patentable for at least the reasons given above with respect to claim 1.

Claim 2 is also patentable over Johnson because Johnson does not teach an encryption apparatus including means for removing an influence of the mask a from intermediate bit data masked by a masking means for at least the same reasons as

given above with respect to claim 1. Thus, Applicants respectfully deem claim 2 allowable over Johnson as well.

Claim 5 depends from claim 2 and thus is patentable for at least the reasons given above with respect to claim 2.

Claim 3 is also patentable over Johnson because Johnson does not teach an encryption apparatus including means for removing an influence of the mask a from an output from a data translation means which is masked by a masking means for at least the same reasons as given above with respect to claim 1. Thus, Applicants respectfully deem claim 3 allowable over Johnson as well.

Claims 6 and 7 depend from claim 3 and thus are patentable for at least the reasons given above with respect to claim 3.

Claim 12 is patentable over Johnson because Johnson does not teach a decryption apparatus including means for masking bits dependent on a ciphertext within the apparatus with mask patterns selected by a selection means. This is because Johnson is directed to solving a particular problem with public key encryption systems that use a public elliptic curve key. (col. 1, ll. 42-62). The method of key encryption taught by Johnson includes generating a masked plaintext block and then encrypting only a portion of that masked plaintext block. (col. 2, ll. 16-37). A ciphertext is then generated from the encrypted portion of the masked plaintext block and the remaining portion of the masked plaintext block. *Id.* The ciphertext, including both the encrypted and unencrypted portions, is then transmitted to a recipient, who reverses the process to recover the original plaintext block. *Id.* Fig. 6 of Johnson shows the process for recovering the original plaintext block, including unmasking procedure 630. Thus,

Johnson teaches a system in which masking of the plaintext occurs at the transmission side (encrypting side) and the unmasking occurs at the receiving side (decrypting side), but not both at the same side. Accordingly, because Johnson does not teach a decryption apparatus including means for masking bits dependent on a ciphertext within the apparatus with mask patterns selected by a selection means, Applicants respectfully deem claim 12 allowable over Johnson as well.

Claims 15 and 19, depend from claim 12 and thus are patentable for at least the reasons given above with respect to claim 12.

Claim 13 is also patentable over Johnson because Johnson does not teach a decryption apparatus including means for masking intermediate bit data within the apparatus with mask patterns selected by a selection means for at least the same reasons as given above with respect to claim 12. Thus, Applicants respectfully deem claim 13 allowable over Johnson as well.

Claims 16 and 20 depend from claim 13 and thus are patentable for at least the reasons given above with respect to claim 13.

Claim 14 is also patentable over Johnson because Johnson does not teach a decryption apparatus including means for masking an input to a data translation means with mask patterns selected by a selection means for at least the same reasons as given above with respect to claim 12. Thus, Applicants respectfully deem claim 14 allowable over Johnson as well.

Claim 18 depends from claim 14 and thus is patentable for at least the reasons given above with respect to claim 14.

Claim 23 is also patentable over Johnson because Johnson does not teach an encryption method including removing an influence of a mask a from a ciphertext before the ciphertext is output for at least the same reasons as given above with respect to claim 1. Thus, Applicants respectfully deem claim 23 allowable over Johnson as well.

Claims 26 depends from claim 23 and thus is patentable for at least the reasons given above with respect to claim 23.

Claim 24 is also patentable over Johnson because Johnson does not teach an encryption method including removing an influence of a mask a from masked intermediate bit data for at least the same reasons as given above with respect to claim 1. Thus, Applicants respectfully deem claim 24 allowable over Johnson as well.

Claim 27 depends from claim 24 and thus is patentable for at least the reasons given above with respect to claim 24.

Claim 25 is also patentable over Johnson because Johnson does not teach an encryption method including removing an influence of the mask a from a masked output from a data translation step for at least the same reasons as given above with respect to claim 1. Thus, Applicants respectfully deem claim 25 allowable over Johnson as well.

Claims 28 and 29 depend from claim 25 and thus are patentable for at least the reasons given above with respect to claim 25.

Claim 34 is also patentable over Johnson because Johnson does not teach a decryption method including masking bits dependent on a ciphertext within the method with selected mask patterns for at least the same reasons as given above with respect to claim 12. Thus, Applicants respectfully deem claim 34 allowable over Johnson as well.

Claims 37, 41, and 42 depend from claim 34 and thus are patentable for at least the reasons given above with respect to claim 34.

Claim 35 is also patentable over Johnson because Johnson does not teach a decryption method including masking intermediate bit data within the method with selected mask patterns for at least the same reasons as given above with respect to claim 12. Thus, Applicants respectfully deem claim 35 allowable over Johnson as well.

Claim 38 depends from claim 35 and thus is patentable for at least the reasons given above with respect to claim 35.

Claim 36 is also patentable over Johnson because Johnson does not teach a decryption method including masking an input to a data translation step with selected mask patterns for at least the same reasons as given above with respect to claim 12. Thus, Applicants respectfully deem claim 36 allowable over Johnson as well.

Claims 39 and 40 depend from claim 36 and thus are patentable for at least the reasons given above with respect to claim 36.

Claim 45 is also patentable over Johnson because Johnson does not teach a computer-readable program code means for converting a plaintext block into a ciphertext block including computer-readable code means for causing a computer to remove an influence of the mask a from a ciphertext before the ciphertext is output for at least the same reasons as given above with respect to claim 1. Thus, Applicants respectfully deem claim 45 allowable over Johnson as well.

Claim 46 is also patentable over Johnson because Johnson does not teach an encryption apparatus including means for removing an influence of the mask a from an output from a data translation means for at least the same reasons as given above with

respect to claim 1. Thus, Applicants respectfully deem claim 46 allowable over Johnson as well.

Claims 47 and 48 depend from claim 46 and thus are patentable for at least the reasons given above with respect to claim 46.

2. Rejection of claims 10, 11, 21, 22, 32, 33, 43, 44, 49, and 50

Applicants respectfully traverse the rejection of claims 10, 11, 21, 22, 32, 33, 43, 44, 49, and 50 under U.S.C. § 103(a) as being unpatentable over Johnson in view of Adams. Applicants respectfully submit that Johnson, even when combined with Adams, does not teach or suggest the claimed subject matter. This is because, as noted above, claims 10 and 11 depend from claim 1, and Johnson does not teach or suggest an encryption apparatus including means for removing an influence of a mask a from a ciphertext before the ciphertext is output, as recited in claim 1. Adams does not cure the deficiency of teachings of Johnson. Adams is directed to constructing large substitution boxes for use in improving the security of symmetric block ciphers (col. 1, ll. 10-14). Adams, however, does not teach or suggest an encryption apparatus including means for removing an influence of a mask a from a ciphertext before the ciphertext is output, as recited in claim 1. Thus, claims 10 and 11, which depend from claim 1, are patentable over Johnson and Adams.

Claims 21 and 22 depend from claim 12 and are patentable even when Johnson is combined with Adams, because these two references do not teach or suggest a decryption apparatus including means for masking bits dependent on a ciphertext within the apparatus with mask patterns selected by a selection means for at least the reasons

discussed above with respect to claim 12. Thus, claims 21 and 22, which depend from claim 12, are patentable over Johnson and Adams.

Claims 32 and 33 depend from claim 23 and are patentable even when Johnson is combined with Adams, because these two references do not teach or suggest an encryption method including removing an influence of a mask a from a ciphertext before the ciphertext is output for at least the reasons discussed above with respect to claims 1, 10, 11, and 23. Thus, Applicants respectfully deem claims 32 and 33 patentable over Johnson and Adams.

Claims 43 and 44 depend from claim 34 and are patentable even when Johnson is combined with Adams, because these two references do not teach or suggest a decryption method including masking bits dependent on a ciphertext within the method with selected mask patterns for at least the same reasons as given above with respect to claims 12 and 34. Thus, Applicants respectfully deem claims 43 and 44 patentable over Johnson and Adams.

Claims 49 and 50 depend from claim 46 and are patentable even when Johnson is combined with Adams, because these two references do not teach or suggest an encryption apparatus including means for removing an influence of the mask a from an output from a data translation means for at least the same reasons as given above with respect to claims 1, 10, 11, and 46. Thus, Applicants respectfully deem claims 49 and 50 patentable over Johnson and Adams.

In view of the foregoing remarks, Applicants respectfully request reconsideration and reexamination of this application and the timely allowance of the pending claims.

Please grant any extensions of time required to enter this response and charge any additional required fees to our deposit account 06-0916.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: June 28, 2004

By: _____
Ranjeev K. Singh
Reg. No. 47,093